

Title (en)

Method for personalisation of a secure element (SE) and computer system

Title (de)

Verfahren zur Personalisierung eines Secure Elements (SE) und Computersystem

Title (fr)

Procédé de personnalisation d'un élément sécurisé (Secure Element SE) et système informatique

Publication

**EP 2752785 A1 20140709 (DE)**

Application

**EP 13192288 A 20131111**

Priority

DE 102012224083 A 20121220

Abstract (en)

The method involves storing personalization information in a secure element (158) by reading personalization information from ID token (106), generating a nonce by ID provider computer system (136) for personalization information, storing nonce in a database, writing data read from ID token personalization information and/or derived value and nonce over network to secure element through legitimate ID provider computer system. The data stored in personalization information is verified and personalized secure elements are activated for use by a terminal program. An independent claim is included for a computer system.

Abstract (de)

Die Erfindung betrifft ein Verfahren zur Personalisierung eines Secure Element (158) mithilfe eines ID-Tokens (106), wobei der ID-Token einen elektronischen Speicher (118) mit einem geschützten Speicherbereich (124, 162) aufweist, in dem eine Personalisierungsinformation gespeichert ist, wobei ein Zugriff auf den geschützten Speicherbereich nur über einen Prozessor (128) des ID-Tokens möglich ist, und wobei der ID-Token eine Kommunikations-Schnittstelle (108) zur Kommunikation mit einem Lesegerät nach einem ersten Datenübertragungsstandard aufweist, wobei das Secure Element einen elektronischen Speicher (118') mit einem geschützten Speicherbereich (124', 162') aufweist, wobei ein Zugriff auf den geschützten Speicherbereich nur über einen Prozessor (128') des Secure Elements möglich ist, und wobei das Secure Element eine Kommunikations-Schnittstelle (164) zur Kommunikation mit dem Lesegerät nach einem zweiten Datenübertragungsstandard aufweist, mit folgenden Schritten: a) Auslesen der Personalisierungsinformation aus dem ID-Token durch ein ID-Provider-Computersystem (136) über ein Netzwerk (116), b) Schreiben der aus dem ID-Token ausgelesenen Personalisierungsinformation über das Netzwerk in das Secure Element durch das ID-Provider-Computersystem.

IPC 8 full level

**G06F 21/34** (2013.01); **H04L 29/06** (2006.01); **H04L 29/08** (2006.01)

CPC (source: EP)

**G06F 21/34** (2013.01); **H04L 63/0853** (2013.01); **H04L 63/0492** (2013.01); **H04L 67/306** (2013.01)

Citation (applicant)

- DE 102008000067 B4 20091231 - BUNDESDRUCKEREI GMBH [DE]
- DE 102008040416 A1 20100121 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009001959 A1 20101007 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009027676 A1 20110120 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009027681 A1 20110120 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009027682 A1 20110120 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009027686 A1 20110120 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009027723 A1 20110127 - BUNDESDRUCKEREI GMBH [DE]
- DE 102009046205 A1 20110512 - BUNDESDRUCKEREI GMBH [DE]
- DE 102010028133 A1 20111027 - BUNDESDRUCKEREI GMBH [DE]
- DE 102011084728 A1 20130418 - BUNDESDRUCKEREI GMBH [DE]
- DE 102011089580 B3 20130425 - AGETO INNOVATION GMBH [DE], et al
- DE 102012215630 A 20120904
- DE 102012201209 A1 20130801 - AGETO INNOVATION GMBH [DE], et al
- DE 3523237 A1 19870102 - SIEMENS AG [DE]
- DE 19507043 A1 19960905 - DEUTSCHE TELEKOM AG [DE]
- DE 19507044 C2 20000406 - DEUTSCHE TELEKOM AG [DE]
- DE 19850307 C2 20020801 - T MOBILE DEUTSCHLAND GMBH [DE]
- EP 0730253 B1 20030618 - DEUTSCHE TELEKOM AG [DE]
- DE 102007008652 A1 20080828 - BUNDESDRUCKEREI GMBH [DE]
- DE 102007008651 A1 20080828 - BUNDESDRUCKEREI GMBH [DE]
- "hierzu U-Prove-Technology Overview V1.1", 2011, MICROSOFT CORPORATION, pages: 18

Citation (search report)

- [IDY] DE 102009046205 A1 20110512 - BUNDESDRUCKEREI GMBH [DE]
- [A] US 2011191829 A1 20110804 - FISCHER JOERG [DE], et al
- [A] "Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften", 24 June 2009 (2009-06-24), XP055117888, Retrieved from the Internet <URL:http://www.bgbl.de/banzxaver/bgbl/text.xav?SID=&start=// \*[@node\_id='170726']&tf=xaver.component.Text\_0&hlf=xaver.component.Hitlist\_0#bgbl109s1346.pdf> [retrieved on 20140514]
- [A] BSI: "Common Criteria Protection Profile Electronic Identity Card (ID\_Card PP)", 15 December 2009 (2009-12-15), pages 1 - 108, XP055117658, Retrieved from the Internet <URL:http://www.commoncriteriaportal.org/files/ppfiles/pp0061b\_pdf.pdf> [retrieved on 20140513]
- [A] JOHN K. WATERS: "RSA Conference: Microsoft Releases Authentication System Under OSP -- Visual Studio Magazine", 3 March 2010 (2010-03-03), XP055118012, Retrieved from the Internet <URL:http://visualstudiomagazine.com/articles/2010/03/03/microsoft-releases-preview-of-uprove.aspx> [retrieved on 20140514]
- [YA] CHRIS CHAVEZ: "No NFC? No Problem! Thanks to SD Cards Equipped With NFC Transmitters", 1 June 2011 (2011-06-01), pages 1 - 4, XP055079659, Retrieved from the Internet <URL:http://phandroid.com/2011/06/01/no-nfc-no-problem-thanks-to-sd-cards-equipped-with-nfc-transmitters/> [retrieved on 20130917]

Cited by

CN107294988A; CN112434270A

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

DOCDB simple family (publication)

**EP 2752785 A1 20140709; EP 2752785 B1 20150916**; DE 102012224083 A1 20150820

DOCDB simple family (application)

**EP 13192288 A 20131111**; DE 102012224083 A 20121220